

SUWERENNA PLATFORMA CYBERBEZPIECZEŃSTWA

Secure Net Intelligence

Jedna platforma. Moduły dobrane do Twojej firmy.

Chroni wszystko, czym firma komunikuje się ze światem: sieć, WWW, pocztę, AI i obraz z kamer. Działa w Twojej infrastrukturze, więc dane nie opuszczają organizacji.


AiSECLAB


- 1 Podłączamy się**
Sieć, poczta, WWW, modele AI i kamery. Bez wymiany systemów.
- 2 Analizujemy na miejscu**
Modele AI działają na Twoich serwerach. Dane nie wychodzą z firmy.
- 3 Reagujemy i raportujemy**
Blokada, alert dla zespołu, raport dla zarządu i pełny audyt.

PAKIETY

Moduł	Start 10–250 osób	Business 250–2000 osób	Critical infrastruktura krytyczna
Core	● Lite	●	●
Network	—	●	●
Web Gateway	●	●	●
Mail Shield	●	●	●
Sovereign Mail	—	○	●
AI Gateway	○	○	●
Vision	—	●	●

● w pakiecie ○ opcja

DLACZEGO SNI

- 🇵🇱 Polski producent i kod**
AiSECLAB z Warszawy. Pełny dostęp do kodu źródłowego, bez czarnych skrzynek.
- 🔒 Dane zostają u Ciebie**
Instalacja lokalna, chmura prywatna lub praca w pełni offline.
- 🔌 Działa z tym, co masz**
M365, Google Workspace, Twoje modele AI i Twoje kamery. Bez wymiany systemów.
- 📄 Wspiera wymogi KSC i NIS2**
Raporty, pełny audyt i dane do zgłoszeń incydentów. Szkolenia zarządu.

ZAUFALI NAM

NASK PIB · Policja Polska · największa sieć convenience w Polsce · Sąd Okręgowy w Zielonej Górze · Ogólnopolska Sieć Edukacyjna

JAK ZACZĄĆ

Warsztat 90 min → Pilotaż → Wdrożenie

KONTAKT

info@aiseclab.com
aiseclab.com

MODUŁ 01 • FUNDAMENT PLATFORMY

SNI Core

Serce każdego wdrożenia. Uruchamia modele AI, zapisuje wyniki wszystkich modułów i pokazuje je w jednym polskim panelu z pełną kontrolą dostępu.

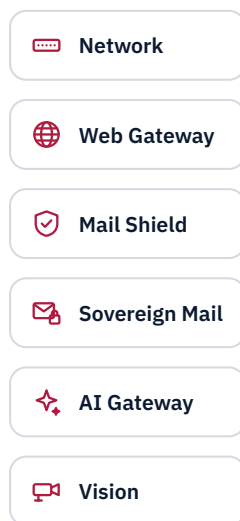
“

Chcę widzieć wszystko w jednym miejscu i mieć dowody na każdą kontrolę.

TAK MÓWI KLIENT

JAK TO DZIAŁA

MODUŁY PLATFORMY

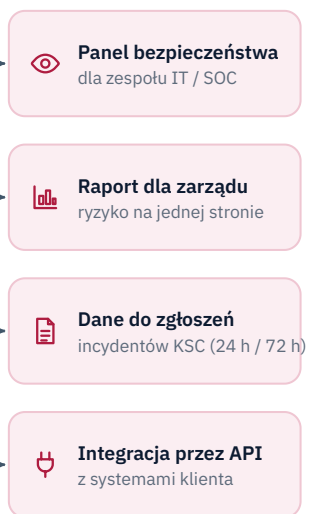


SNI CORE

działa u Ciebie, także bez internetu



EFEKT



KROK 1

Zbiera

Każdy moduł przekazuje do Core swoje zdarzenia: z sieci, WWW, poczty, AI i kamer.

KROK 2

Analizuje

AI Model Server uruchamia modele równolegle, także własne modele klienta.

KROK 3

Zapisuje

Baza analityczna przechowuje zdarzenia z próbką, kontekstem i pełnym audytem.

KROK 4

Pokazuje

Dashboardy dla zespołu, raporty dla zarządu i dane do zgłoszeń incydentów.

PRZYKŁAD Z ŻYCIA

Po incydencie zarząd pyta, co się stało i kogo to dotyczy. **Zespół odtwarza przebieg zdarzeń w jednym panelu**, zamiast zbierać logi z kilku systemów, i od razu ma dane do zgłoszenia.

CO ZAWIERA

- **AI Model Server:** wydajna inferencja, setki kopii modeli
- **Baza analityczna:** szybkie wyszukiwanie, język polski
- **Dashboardy:** dowolne widoki i uprawnienia według ról
- **Konsola:** aktualizacje, skalowanie i konfiguracja

EFEKT DLA FIRMY

- Jeden panel zamiast kilku narzędzi
- Gotowe raporty dla zarządu i na potrzeby KSC
- Dowody zamiast domysłów przy incydencie lub kontroli
- Skalowanie od jednego serwera do klastra

W PAKIETACH



W każdym wdrożeniu. W pakiecie Start w lżejszej wersji na jednym serwerze.

Instalacja: serwerownia klienta, chmura prywatna lub tryb offline (air-gapped).

MODUŁ 02 • BEZPIECZEŃSTWO SIECI

SNI Network

Analizuje cały ruch w sieci IT, wszystkie protokoły, z zewnątrz i od środka. Reguły, modele statystyczne i głębokie uczenie wykrywają to, czego nie widzą klasyczne zabezpieczenia.

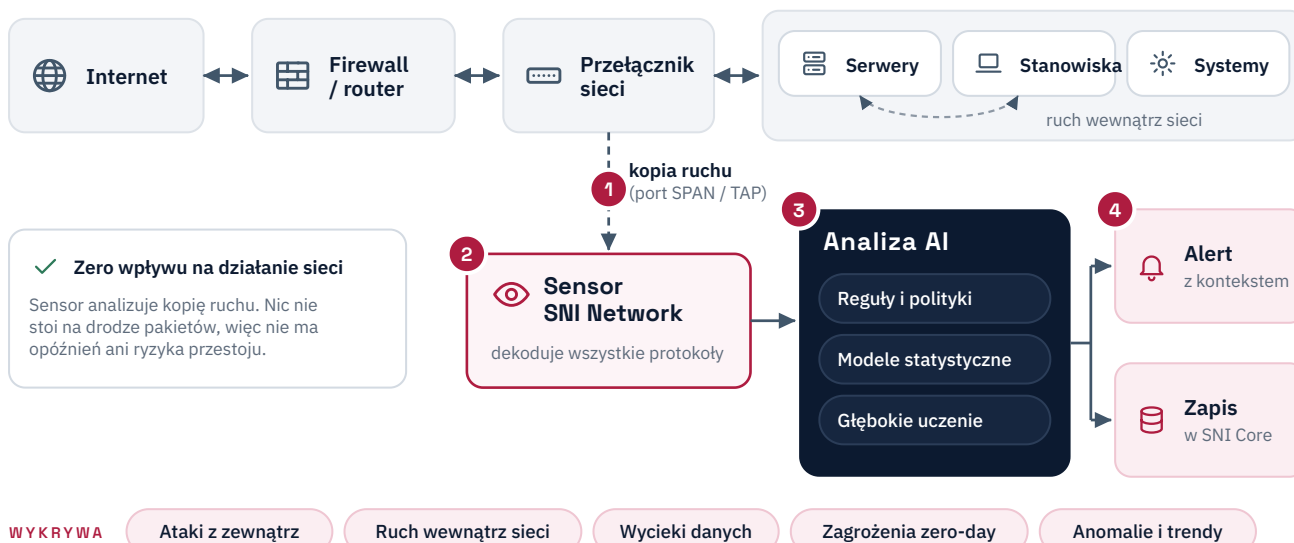
“

Nie wiem, co naprawdę dzieje się w mojej sieci.

TAK MÓWI KLIENT

JAK TO DZIAŁA

TWOJA SIEĆ DZIAŁA BEZ ZMIAN



KROK 1 Kopia ruchu

Przetącnik przekazuje kopię ruchu do sensora. Sieć działa dokładnie jak dotąd.

KROK 2 Rozpoznanie

Sensor dekoduje protokoły i buduje pełny obraz komunikacji w firmie.

KROK 3 Analiza AI

Reguły, statystyka i głębokie uczenie oceniają każde połączenie.

KROK 4 Reakcja

Alert z kontekstem trafia do zespołu, a zdarzenie do SNI Core.

PRZYKŁAD Z ŻYCIA

Komputer w księgowości w nocy łączy się z nieznanym serwerem i wysyła duże pliki. **Sensor wykrywa anomalie, a zespół dostaje alert z kontekstem:** która maszyna, dokąd i ile danych.

CO WYKRYWA

- Ataki i skanowanie z zewnątrz
- Nietypowy ruch wewnątrz sieci
- Wycieki danych
- Nieznane zagrożenia (zero-day)
- Anomalie i trendy w czasie

EFEKT DLA FIRMY

- Pełna widoczność sieci IT
- Czas reakcji skrócony z minut do sekund
- Dane do zgłoszeń incydentów wymaganych przez KSC
- Od jednego biura po grupę kapitałową

W PAKIETACH

Start

Business
w pakiecie

Critical
w pakiecie

Wdrożenie referencyjne:

Ogólnopolska Sieć Edukacyjna (OSE).

Zakres: sieć IT (biurowa, korporacyjna, styk z internetem).

MODUŁ 03 • KONTROLA RUCHU WEBOWEGO

SNI Web Gateway

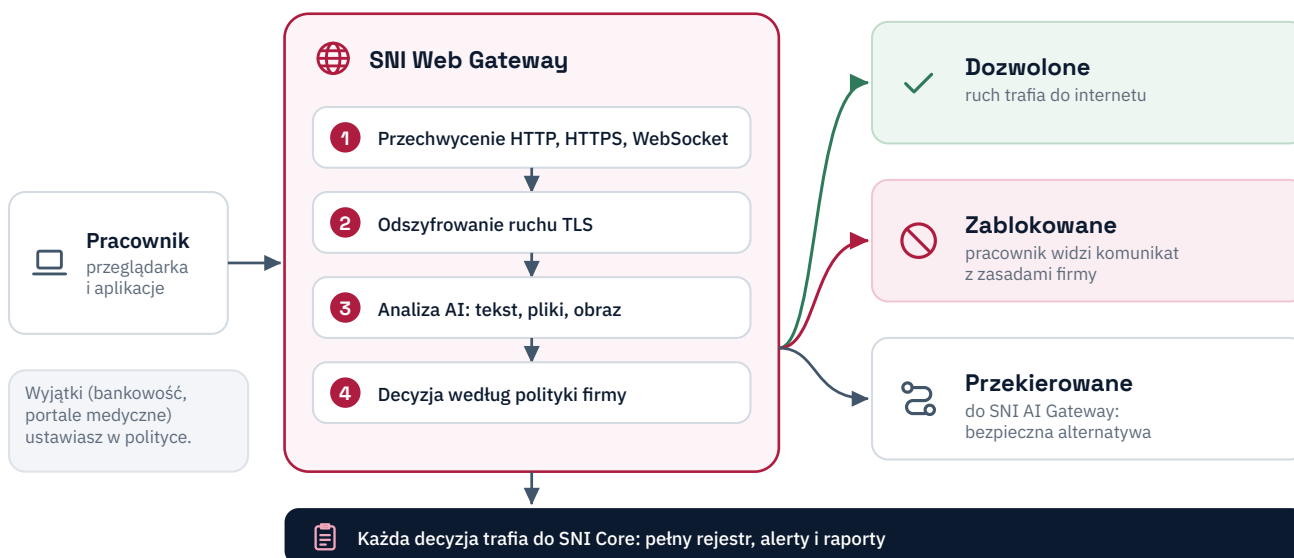
Widzi cały ruch internetowy, także szyfrowany. Zatrzymuje wyciek danych przez przeglądarkę i publiczne chatboty, zanim dane opuszczą firmę.

“

Pracownicy wklejają dane firmy do ChatGPT, a ja się o tym nie dowiem.

TAK MÓWI KLIENT

JAK TO DZIAŁA



KROK 1

Przechwycenie

Ruch HTTP, HTTPS i WebSocket przechodzi przez bramę SNI.

KROK 2

Odszyfrowanie

Brama odszyfrowuje ruch TLS, więc widzi treść, a nie tylko adres.

KROK 3

Analiza AI

Modele oceniają teksty, dokumenty, obrazy i wideo w czasie rzeczywistym.

KROK 4

Decyzja

Przepuść, zablokuj lub przekieruj. Pracownik dostaje wyjaśnienie.

PRZYKŁAD Z ŻYCIA

Pracownik wkleja do publicznego chatbota umowę z danymi klienta. **System blokuje operację, informuje pracownika o zasadach i rejestruje zdarzenie.**

CO ROBI

- Blokuje wysyłanie danych do publicznych AI
- Chroni przed wyciekiem i kradzieżą danych (DLP)
- Wykrywa nieznanne zagrożenia
- Tworzy czarne i białe listy automatycznie
- Polityki dla działów i grup

EFEKT DLA FIRMY

- Dane firmy zostają w firmie
- Zasady egzekwowane automatycznie
- Pracownik wie, dlaczego operację zablokowano
- Pełny rejestr zdarzeń dla zarządu

W PAKIETACH

- Start** w pakiecie
- Business** w pakiecie
- Critical** w pakiecie

Referencje: NASK PIB, Ogólnopolska Sieć Edukacyjna (OSE).

Najlepiej w parze z AI Gateway: blokujemy publiczne AI i od razu dajemy bezpieczną alternatywę.

MODUŁ 04 • OCHRONA ISTNIEJĄCEJ POCZTY

SNI Mail Shield

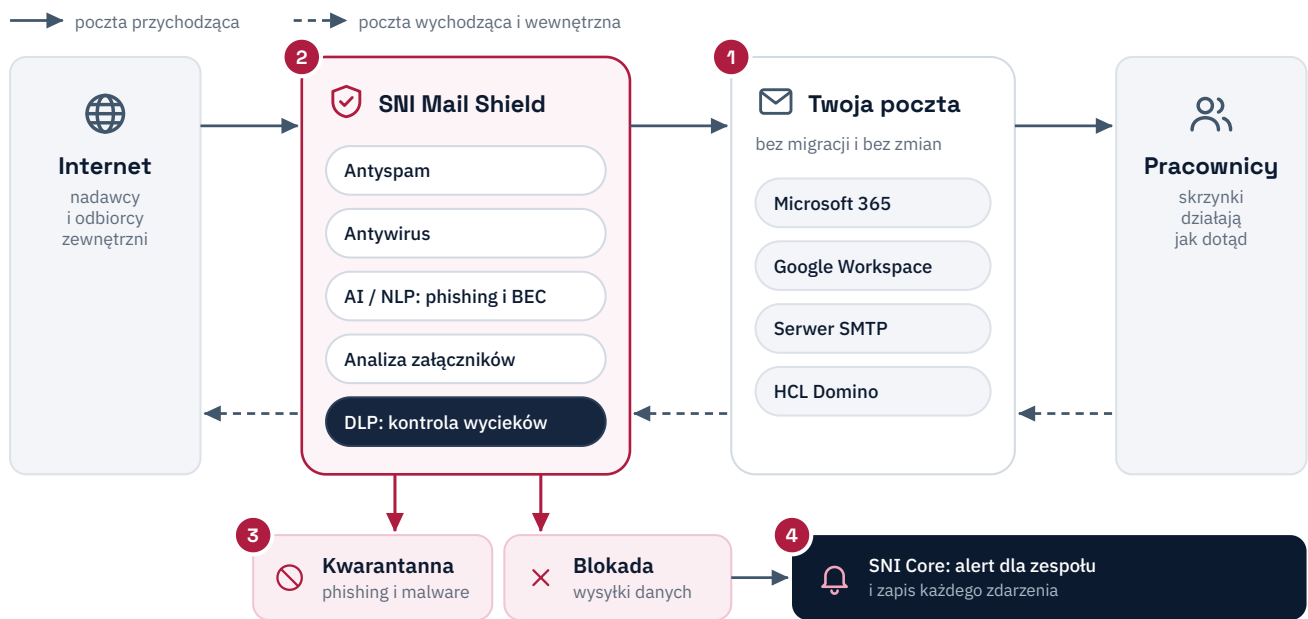
Tarcza AI dla poczty, którą firma już ma. Analizuje wiadomości przychodzące, wychodzące i wewnętrzne razem z załącznikami, bez wymiany systemu pocztowego.

“

Boję się fałszywego maila od prezesa, a nie chcę zmieniać poczty.

TAK MÓWI KLIENT

JAK TO DZIAŁA



KROK 1

Połączenie

Integracja z Microsoft 365, Google Workspace, SMTP lub HCL Domino.

KROK 2

Analiza

Antyspam, antywirus i modele NLP oceniają nadawcę, treść i załączniki.

KROK 3

Decyzja

Dostarcz, przenieś do kwarantanny lub zablokuj zgodnie z polityką.

KROK 4

Raport

Alert dla zespołu i zapis każdego zdarzenia w SNI Core.

PRZYKŁAD Z ŻYCIA

Księgowa dostaje e-mail „od prezesa” z pilną prośbą o przelew. Modele NLP rozpoznają podszycie, wiadomość trafia do kwarantanny, a zespół bezpieczeństwa dostaje alert.

CO ZATRZYMUJE

- Phishing i wyłudzenia
- Podszywanie się pod zarząd (BEC)
- Złośliwe załączniki i oprogramowanie
- Wycieki w poczcie wychodzącej i wewnętrznej, także w załącznikach i archiwach

EFEKT DLA FIRMY

- Ochrona bez kosztów i ryzyka wymiany systemu
- Szybkie wdrożenie, szybki zwrot
- Mniej udanych ataków na ludzi
- Dowody na każdy incydent

W PAKIETACH

- Start** w pakiecie
- Business** w pakiecie
- Critical** w pakiecie

Referencja: Policja Polska.

Pierwszy krok dla większości firm. Naturalny wstęp do Sovereign Mail.

MODUŁ 05 • SUWERENNA POCZTA

SNI Sovereign Mail

Własna, szyfrowana poczta pod pełną kontrolą organizacji. Serwer stoi tam, gdzie zdecydujesz, klucze należą do Ciebie, a każda operacja na skrzynce zostawia ślad.

“

Chcę wiedzieć, gdzie są nasze wiadomości i kto je czytał.

TAK MÓWI KLIENT

JAK TO DZIAŁA



KROK 1

Szyfrowanie u nadawcy

Wiadomość jest szyfrowana już w przeglądarce, kluczem X.509.

KROK 2

Bezpieczny serwer

Dane są zaszyfrowane w transmisji i w spoczynku, na Twoim serwerze.

KROK 3

Ochrona i DLP

Wbudowana tarcza AI i polityki DLP działają także na poczcie szyfrowanej.

KROK 4

Audyt

Rejestr pokazuje kto, co i kiedy zrobił ze skrzynką lub wiadomością.

PRZYKŁAD Z ŻYCIA

Pracownik wysłał bazę klientów na prywatną skrzynkę. Wiadomość zostaje zablokowana, pracownik dostaje wyjaśnienie, a zespół bezpieczeństwa zgłoszenie z pełnym śladem.

CO DAJE

- Pełna kontrola nad danymi i kluczami
- Szyfrowanie end-to-end
- Audyt: odczyt, przekazanie, usunięcie, zmiana uprawnień, dostęp administratora
- Nowoczesny interfejs na komputerze i telefonie

EFEKT DLA FIRMY

- Cyfrowa suwerenność komunikacji
- Dowody gotowe na kontrolę i spór
- Migracja bez przestojów i bez zmiany nawyków zespołu

W PAKIETACH

Start

Business

opcja

Critical

w pakiecie

Referencja: Policja Polska.

Model wdrożenia: u siebie, chmura prywatna lub hybryda. Zmiana modelu w dowolnym momencie.

MODUŁ 06 • BEZPIECZNA SZTUCZNA INTELIGENCJA

SNI AI Gateway

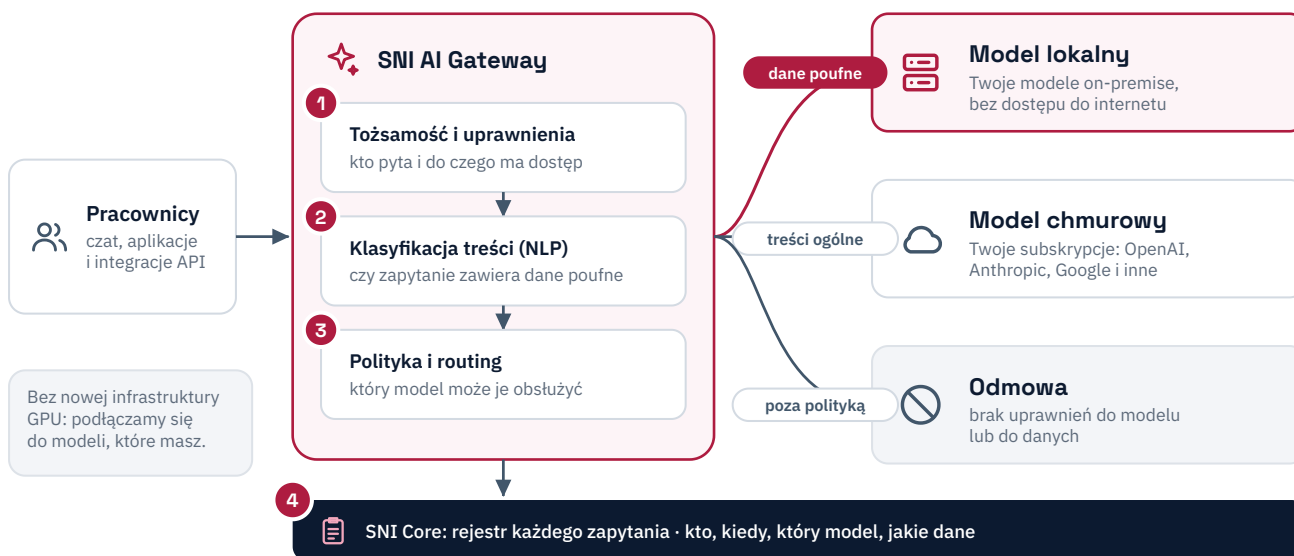
Jedna brama do wszystkich modeli AI, z których korzysta firma, lokalnych i chmurowych. Zespół pracuje z AI, a organizacja decyduje, jakie dane i gdzie mogą trafić.

“

Chcę, żeby zespół używał AI, ale bez wypływu tajemnic firmy.

TAK MÓWI KLIENT

JAK TO DZIAŁA



KROK 1 Logowanie

Pracownik korzysta z AI przez bramę, z własnym kontem i uprawnieniami.

KROK 2 Klasyfikacja

Modele NLP rozpoznają, czy zapytanie zawiera dane poufne.

KROK 3 Routing

Poufne do modelu lokalnego, ogólne do chmury, reszta zgodnie z polityką.

KROK 4 Rozliczalność

Każde zapytanie jest zapisane w SNI Core: kto, kiedy, który model.

PRZYKŁAD Z ŻYCIA

Analitik prosi AI o streszczenie umowy z kontrahentem. **Brama rozpoznaje dane poufne i kieruje zapytanie do modelu lokalnego.** Pytanie o ogólny trend rynkowy trafią do modelu w chmurze.

CO DAJE

- Działa z modelami, które firma już ma: on-premise i w chmurze
- Izolowane modele lokalne do informacji poufnych
- Jedna polityka: kto, z jakich modeli i do czego
- Pełna rozliczalność zapytań

EFEKT DLA FIRMY

- Produktywność bez utraty kontroli nad wiedzą firmy
- Koniec szarej strefy AI
- Szybkie wdrożenie, bez nowej infrastruktury GPU

W PAKIETACH

- Start
opcja
- Business
opcja
- Critical**
w pakiecie

Nie sprzedajemy modeli. Dajemy kontrolę nad tymi, z których korzystasz: OpenAI, Anthropic, Google oraz modelami lokalnymi.

MODUŁ 07 • WIZYJNA AI (OPTIMIND)

SNI Vision

Zamienia kamery, które firma już ma, w system wykrywania zdarzeń. Inteligencja działa na platformie, a nie w kamerze, więc alarmów fałszywych jest mniej, a rozwój nie wymaga wymiany sprzętu.

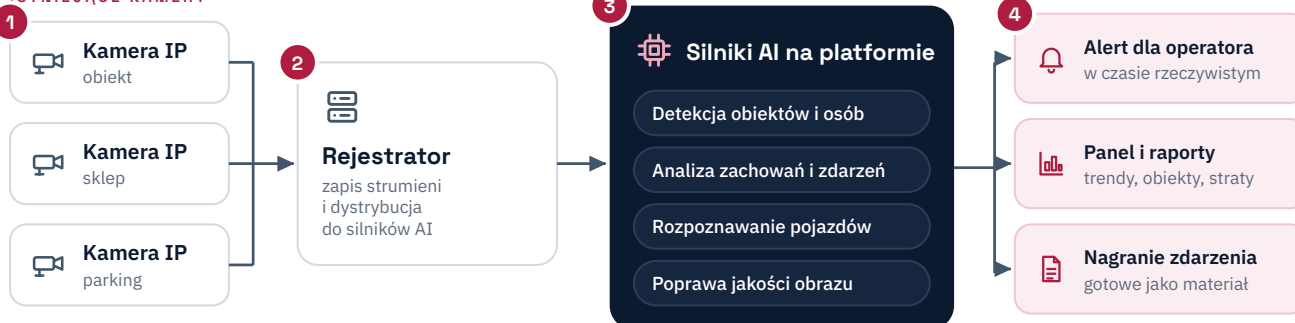
“

Mam setki kamer, ale nikt nie patrzy w monitory.

TAK MÓWI KLIENT

JAK TO DZIAŁA

ISTNIEJĄCE KAMERY



PAKIETY ZASTOSOWAŃ • DOBIERASZ WEDŁUG BRANŻY



Infrastructure

włamania, wandalizm, bójki, pożary, nieprawidłowe parkowanie



Retail

puste półki, kradzieże, kasy samoobsługowe, strefa bistro



Traffic

tablice rejestracyjne, marki, modele, kolory i typy pojazdów



Enhance

poprawa jakości nagrań i zdjęć z zachowaniem integralności danych

KROK 1

Podłączenie

Istniejące kamery IP przekazują obraz do platformy.

KROK 2

Rejestracja

Rejestrator zapisuje strumienie i rozdziela je na silniki AI.

KROK 3

Analiza

Modele wykrywają zdarzenia w czasie rzeczywistym.

KROK 4

Reakcja

Alert dla operatora, nagranie zdarzenia i raport w panelu.

PRZYKŁAD Z ŻYCIA

Kamera nad kasą samoobsługową rejestruje produkt, którego klient nie zeskanował. **Operator dostaje alert w czasie rzeczywistym** razem z nagraniem zdarzenia.

DLACZEGO NA PLATFORMIE

- Standardowe kamery, które już są w obiekcie
- Wyższa skuteczność, mniej fałszywych alarmów
- Algorytmy rozwijane bez dotykania sprzętu
- Skala od 1 do ponad 100 000 kamer

EFEKT DLA FIRMY

- Mniejsze straty i wyższa sprzedaż w handlu
- Niższe koszty ochrony obiektów
- Materiał dowodowy, który obroni się w sądzie
- Pilotaż w jednym obiekcie, rozbudowa w swoim tempie

W PAKIETACH

Start

—

Business

w pakiecie

Critical

w pakiecie

Referencje: największa sieć convenience w Polsce, Policja Polska, Sąd Okręgowy w Zielonej Górze.